Cisco ASA 5500 Series Unified Communications Deployments

Cisco® Unified Communications solutions unify voice, video, data, and mobile applications on fixed and mobile networks, enabling easy collaboration every time, from any workspace.

Overview

Cisco Unified Communications products can help businesses of all sizes streamline operations, increase employee productivity, optimize communications, and enhance customer care. Because protecting a unified-communications-based network from attacks is crucial to maintaining business continuity and integrity, Cisco has built security features into its unified communications products, and augments them with the Cisco ASA 5500 Series Adaptive Security Appliances.

Cisco ASA 5500 Series Adaptive Security Appliances are ideal for small businesses, branch offices, enterprises, and mission-critical data center environments. These multifunction appliances deliver market-leading voice and video security services for unified communications, including robust firewall, full-featured IP Security (IPsec) and Secure Sockets Layer (SSL) VPN, intrusion prevention, and content security features. For unified communications deployments, these platforms can protect up to 30,000 phones and deliver application inspection for a broad range of unified communications protocols, including Skinny Client Control Protocol (SCCP), Session Initiation Protocol (SIP), H.323, Media Gateway Control Protocol (MGCP), Computer Telephony Interface Quick Buffer Encoding (CTIQBE), Real-Time Transport Protocol (RTP), and Real-Time Transport Control Protocol (RTCP).

Cisco ASA 5500 Series Unified Communications Features

Cisco ASA 5500 Series Adaptive Security Appliances are designed to secure real-time unified communications applications such as voice and video. These appliances protect all of the critical elements of your unified communications deployment (network infrastructure, call-control platforms, IP endpoints, and unified communications applications). They deliver several security features that complement the embedded security within the unified communications system, providing additional layers of protection. These features include:

- Access control: Dynamic and granular policy access control prevents unauthorized access to unified communications services.
- Threat prevention: Built-in threat prevention protects the unified communications infrastructure from attempts to exploit the system.
- Network security policy enforcement: Effective unified communications policies for applications and users are created and administered.
- Voice encryption services: Cisco Transport Layer Security (TLS) proxy can help customers maintain their security policies while encrypting signaling and media.
- Perimeter security services for unified communications: In addition to SSL and IPsec VPN services, phone proxy, mobility proxy, and presence federation, security services allow businesses to securely extend communications services to remote users, mobile solutions, and business-to-business collaboration.

Access Control

Access control is a basic security function that allows only authorized access to resources and services within a system. In a unified communications context, this control is often related to providing network-layer access control to the Cisco Unified Communications Manager and other application servers as a first line of defense against attack.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Restricting access to the Cisco Unified Communications Manager servers significantly reduces the risk of an attacker probing the system for vulnerabilities or exploiting access through unauthorized network channels.

Cisco ASA 5500 Series Adaptive Security Appliances are voice- and video-aware, and can inspect and apply policy to the protocols (SIP, SCCP, H.323, and MGCP) used in modern unified communications. Older network access control mechanisms, such as access control lists (ACLs), cannot process these more complex protocols with the granularity and dynamism required by most organizations.

Unlike traditional data applications, unified communications protocols dynamically negotiate how to communicate by exchanging port information within the signaling control channel. Static access control mechanisms such as ACLs cannot track which ports to open and must therefore apply weak access controls, limiting the ability to implement effective access policies.

Cisco ASA 5500 Series Adaptive Security Appliances can dynamically track the authorized connections that should be opened, and then close the connections as soon as the session has ended. This level of control, combined with other intelligent services such as voice-protocol-aware Network Address Translation (NAT), distinguishes the Cisco ASA 5500 Series from older platforms that are not suited to the requirements of modern unified communications protocols.

Threat Prevention

The Cisco ASA 5500 Series protects Cisco Unified Communications applications from a range of common attacks that can threaten the integrity and availability of your system. These attacks include call eavesdropping, user impersonation, toll fraud, and denial of service (DoS). Many of these attacks (in particular, DoS) can be launched by sending malformed protocol packets to attack your unified communications call-control systems and applications. Cisco ASA 5500 Series appliances perform protocol conformance and compliance checking on traffic destined to critical unified communications servers. For example, the appliances can help ensure that media flowing through the appliance is truly voice media (RTP), or prevent attackers from sending malicious voice signaling that could crash your call-control systems. By helping to ensure that signaling and media comply with standard RFCs, the Cisco ASA 5500 Series provides an effective first line of defense for your critical systems.

In addition to checking protocol conformance, the multifunction security services of the Cisco ASA 5500 Series can be extended to provide intrusion prevention services. The Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Module (AIP SSM) applies hardware-based intrusion-prevention-system (IPS) features to inbound traffic to stop known attacks against unified communications call-control and application servers. A set of unified communications IPS signatures is available to protect against Cisco Unified Communications Manager and Cisco Unified Communications Manager Express Product Security Incident Response Team (PSIRT) vulnerabilities, giving your IT administrators immediate protection without needing to patch unified communications servers right away. The combination of protocol conformance and intrusion prevention provides a robust network-layer defense against common unified communications threats.

Network Security Policy Enforcement

Your unified communications deployments are probably subject to the security policy requirements established by your organization’s security department. With the sophisticated unified communications security features of the Cisco ASA 5500 Series, your organization can apply granular, application-layer policies to the unified communications traffic to meet security compliance requirements. For example, your business can permit or deny calls from specific callers or domains, or can apply specific black lists or white lists. As another example, you can extend your network policies to endpoints and applications to allow only calls from phones registered to the call-control server or to deny applications such as instant messaging over SIP.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Voice and Video Encryption Services

For compliance or security policy reasons, your organization might be required to provide confidentiality to voice and video traffic. End-to-end encryption often leaves network security appliances “blind” to media and signaling traffic, a situation that can compromise access control and threat prevention security functions. This scenario can result in a lack of interoperability between the firewall and the encrypted voice, leaving your business unable to satisfy both of your critical security requirements.

The Cisco ASA 5500 Series encryption proxy solution offers exceptional support (TLS proxy) for Cisco Unified Communications Systems. It is a trusted device within the Cisco Unified Communications Manager authentication domain: voice and video endpoints can securely authenticate and encrypt traffic. The Cisco ASA 5500 Series appliance, as a proxy, can decrypt these connections, apply the required threat protection and access control, and help ensure confidentiality by reencrypting the traffic onto the Cisco Unified Communications Manager servers. This integration can give your organization the flexibility to deploy all of the required security countermeasures rather than settling for an inadequate subset.

Perimeter Security Services

Perimeter security services include the following:

- SSL and IPsec VPN: The Cisco ASA 5500 Series supports flexible, secure connectivity using SSL or IPsec VPN services that deliver secure, high-speed voice and data communications among multiple office locations or remote users. These appliances support quality-of-service (QoS) features to facilitate reliable, business-quality delivery of latency-sensitive applications such as voice and video. You can apply the QoS policies on a per-user, per-group, per-tunnel, or per-flow basis so that the proper priority and bandwidth restrictions are applied to voice and video flows. In addition, preconnection posture assessment and security checks help ensure that VPN users do not inadvertently bring attacks to the network. The Cisco SSL and IPsec solutions are ideally suited to protecting soft-client unified communications traffic such as Cisco IP Communicator and Cisco Unified Mobile and Personal Communicators.
- Phone proxy: The Cisco ASA phone proxy capability facilitates termination of Cisco SRTP- and TLS-encrypted endpoints for secure remote access. The Cisco ASA phone proxy allows large-scale deployments of secure phones without a large-scale VPN remote-access hardware deployment. End-user infrastructure is limited to just the IP endpoint, without VPN tunnels or hardware. The Cisco ASA phone proxy is the replacement product for the Cisco Unified Phone Proxy.
- Mobility proxy: The Cisco ASA mobility proxy facilitates secure connectivity between the Cisco Unified Mobile Communicator software and the Cisco Unified Mobility Advantage server. The Cisco ASA appliance can intercept the TLS connection between the Cisco Unified Mobile Communicator software and Cisco Unified Mobility Advantage server, and inspect and apply policies to the mobility traffic using a new Multichassis Multilink PPP (MMP) inspection engine. The Cisco ASA appliance is a mandatory component of mobility solutions starting with the Cisco Unified Communications 7.0 systems, and replaces the Cisco Unified Mobility Proxy.
- Presence federation: The Cisco ASA 5500 Series facilitates secure presence federation between Cisco Unified Presence and the Microsoft Office Communications Server (OCS) Presence solutions. This allows two organizations to collaborate more efficiently by sharing presence information about how to best reach and communicate with other users, using the common form of communication that is available. The Cisco ASA 5500 Series Adaptive Security Appliance is a mandatory component of presence federation solutions.

Deployment Topologies

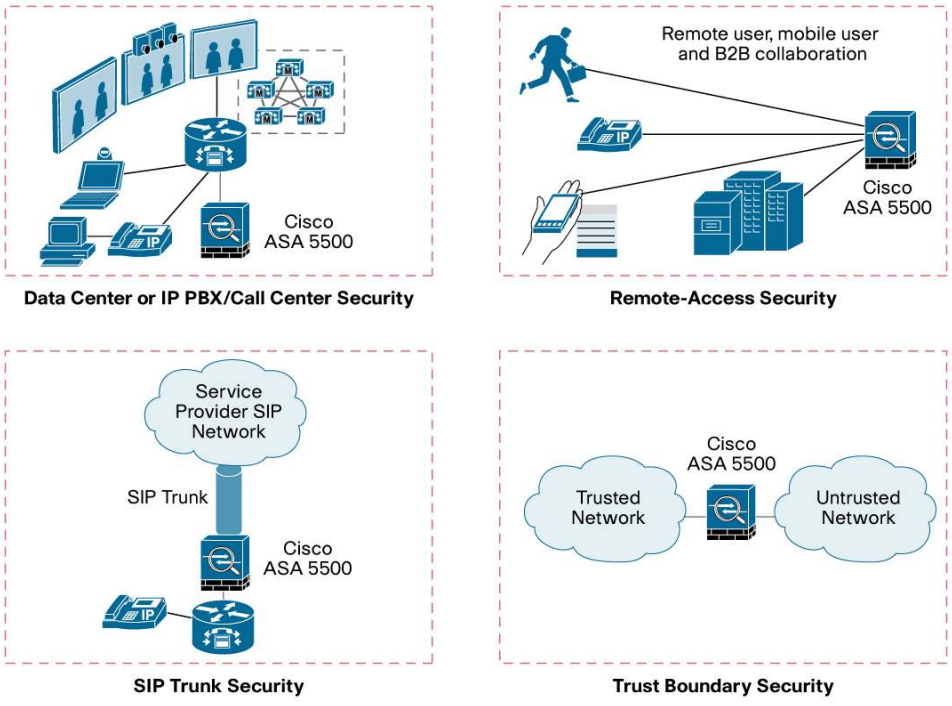
As shown in Figure 1, you can use the Cisco ASA 5500 Series across your network to protect your call-control system, endpoints, applications, and the underlying infrastructure from attacks. These topologies include:

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- Protection of call-control servers: By controlling access from clients to these servers, the Cisco ASA 5500 Series can prevent malicious or unauthorized network connections that could affect performance or availability. By statefully inspecting the connections to ascertain that they meet the access-control policy and that the connection conforms to expected behavior, the Cisco ASA platform provides a first line of defense for a secure unified communications deployment.
- Remote-access security: The Cisco ASA 5500 Series delivers SSL and IPsec VPN, phone proxy, mobility proxy, and presence federation security services to secure teleworker phones, Cisco Unified IP Phones, and third-party phones such as Apple iPhones, mobile phones, and business-to-business federation deployments.
- SIP trunk security: Businesses are migrating to SIP trunk architectures to lower their communication costs. The robust SIP security capabilities of the Cisco ASA 5500 Series provide protection from any attacks through SIP trunks.
- Trusted and untrusted boundaries: You can position the Cisco ASA 5500 Series as a security device between a trusted and untrusted network to help ensure that vulnerabilities from the untrusted network do not affect the trusted network. You can use a Cisco ASA 5500 Series appliance to proxy traffic, or to secure an internal network against external access in a DMZ architecture.

With the range of Cisco ASA 5500 Series models available, your organization has the flexibility to standardize on a single family of security products while positioning specific models to meet different performance needs for every topology or location.

Figure 1. Cisco ASA 5500 Series Deployment Topologies



The Cisco ASA 5500 Series provides a comprehensive suite of voice and video security features for your unified communications network. Table 1 lists the features and benefits.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Table 1. Features and Benefits Summary

Feature	Details
Unified Communications Application Inspection and Control	• Supported protocols include SIP, SCCP, H.323, MGCP, RTP and RTCP, TCP, CTIQBE, and Real Time Streaming Protocol (RTSP).
SIP Application Inspection and Control	• This feature facilitates deep inspection services for SIP traffic for both User Datagram Protocol (UDP)- and TCP-based SIP environments, providing granular control for protection against unified communications attacks. • SIP application inspection and control delivers protocol conformance support for numerous SIP RFCs, including RFC 3261. It delivers SIP state awareness and tracking and the ability to enforce mandatory header fields and absence of forbidden header fields, thus protecting your business from attacks that use malformed packets. • The feature facilitates Network Address Translation (NAT)- and Port Address Translation (PAT)-based address translation support for SIP-based IP phones and applications such as Microsoft Windows Messenger, while delivering advanced services such as call forwarding, call transfers, and more. • This feature supports comprehensive threat defense features such as SIP state awareness and tracking; the ability to rate-limit SIP traffic to prevent DoS attacks, preventing SIP traffic from specific proxies from blocking SIP traffic from rogue proxy servers; and validation of RTP and RTCP for media. • SIP application inspection and control allows your business to configure granular unified communications policies. These include permitting and denying callers and callees by configuring SIP Uniform Resource Identifier (URI) filters and inbound and outbound calls using white lists and black lists. In addition, SIP application inspection and control enables permitting and denying use of applications such as instant messaging over SIP, or permitting and denying specific SIP methods (including user-defined methods).
H.323 Security Services	• H.323 Versions 1-4 along with Direct Call Signaling (DCS) and Gatekeeper Router Control Signaling (GKRCS) provide flexible security integration in a variety of H.323-controlled voice-over-IP (VoIP) environments. • These services support NAT and PAT, including advanced features such as fax over IP (FoIP) using the T.38 protocol, an ITU standard that defines how to transmit FoIP in real time. • These services support threat prevention for H.323 traffic such as restricting call duration, preventing H.225 Registration, Admission, and Status (RAS) packets from arriving out of state, and validation of RTP and RTCP for media. • This can help your business configure granular policies for H.323 services such as filtering on calling and called phone numbers to prevent rogue callers, and restricting services by filtering on specific media types.
SCCP Security Services	• Advanced SCCP inspection services support SCCP applications such as Cisco Unified IP Phones, Cisco Unified Personal Communicator, and Cisco IP Communicator to provide flexible security integration. • These services offer comprehensive threat defense such as the ability to set the maximum SCCP message length to prevent buffer overflow attacks, the ability to tune timeouts for TCP SCCP connections and SCCP audio and video media connections, and validation of RTP and RTCP for media. • The services can help your business configure granular policies for SCCP traffic, such as enforcing only registered phone calls to send traffic through the Cisco ASA appliance and filtering on message IDs to allow or deny specific messages.
MGCP Security Services	• Rich MGCP security services facilitate NAT- and PAT-based address-translation services for MGCP-based connections between media gateways and call agents or media gateway controllers.
RTSP Security Services	• RTSP security services facilitate inspection of RTSP protocols used to control communications between the client and server for streaming applications such as Cisco IP/TV, Apple QuickTime, and RealNetworks RealPlayer. • RTSP security services deliver NAT- and PAT-based address translation services for RTSP media streams to improve support in real-time networking environments.
Fragmented and Segmented Multimedia Stream Inspection	• This feature facilitates inspection of H.323-, SIP-, and SCCP-based voice and multimedia streams that have been fragmented or segmented to prevent against these unique unified communications attacks.
Advanced TCP Security Engine	• The advanced TCP security engine protects your network from several attacks, including SYN flood attacks using SYNC cookies, and protects your network endpoints against protocol fuzzing and retransmission-style time-to-live (TTL) evasion. • This security engine delivers a smart TCP proxy feature that reassembles TCP packets to protect against segment attacks that use multiple TCP packets. • The security engine offers TCP traffic normalization services for additional techniques to detect attacks, including advanced flag and option checking, TCP packet checksum verification, detection of data tampering in retransmitted packets, and more.
RTP and RTCP Inspection Services	• These services provide the ability to inspect RTP and RTCP traffic on media connections opened by the unified communications inspection engines, such as SIP and SCCP connections. • The services can help your business set security policies for RTP and RTCP traffic such as validating conformance to RFC 1889; cross-checking media values between signaling and RTP to validate payload type; and policing of version number, payload type integrity, sequence numbers,

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Details
	and the synchronization source (SSRC).
Threat Prevention	
Intrusion Prevention Services	• The optional Cisco ASA 5500 Series AIP SSM applies intrusion prevention services to protect the unified communications infrastructure and call-control servers from IPS signature-based attacks. The AIP SSM provides IPS services that are optimized for unified communications and support specific unified communications engines such as the H.323 and H.225 inspection engines; it also helps prevent OS attacks on call-control servers. • Unique intrusion prevention capabilities such as anomaly detection, OS fingerprinting capabilities, and risk-rating features provide better context on threats to prevent false positives.
Content Security Services	• These services can help your business implement a gateway-based content-inspection feature to inspect content of email and web traffic. This helps ensure that the unified communications infrastructure is free from viruses, worms, spam, phishing, and malware attacks.
Encryption Services	
TLS Proxy	• TLS proxy addresses encrypted signaling and firewall integration concerns in situations in which encrypted signaling leaves unified communications firewalls unable to dynamically open ports or apply policies. • As a trusted device within the Cisco Unified Communications Manager, the Cisco ASA appliance can intercept the encrypted signaling, mutually authenticate with the endpoint, and decrypt the signaling. After the signaling is decrypted, the appliance retrieves all the necessary signaling information and applies all the inspection and policy enforcement actions. To maintain secure connectivity from end to end, the appliance then initiates a secondary TLS session back to Cisco Unified Communications Manager. The signaling and communications between endpoint and Cisco Unified Communications Manager remain functionally the same, and the firewall can deliver its unified communications security services. • TLS proxy services support both SIP and SCCP endpoints for comprehensive integration with Cisco Unified IP Phones.
Perimeter Security Services	
Phone Proxy	• Phone proxy delivers secure remote access without the need for a remote-access VPN device. It does so by terminating SCCP and SIP Cisco Unified IP Phone endpoints encrypted with TLS or SRTP. Phone proxy supports Cisco Unified Communications Manager mixed and nonsecure modes. You can deploy phone proxy behind an existing firewall or as an integrated firewall or phone proxy appliance.
Mobility Proxy	• Mobile proxy protects Cisco Unified Mobility solutions, and replaces Cisco Unified Mobility Proxy. It incorporates a new inspection engine to validate mobility traffic, including protocol conformance for Cisco Unified Mobile Communicator running on Blackberry, Symbian, and Windows mobile devices.
Presence	• This mandatory federation component of Cisco Unified Presence with Microsoft Presence solutions secures presence information and applies security policies (white list, black list, and protocol conformance) between two organizations.
SSL and IPsec VPN	• Robust encrypted SSL and IPsec VPN services for both unified communications and data traffic offer preconnection posture assessment for endpoints and the ability to apply policies and inspection capabilities to VPN traffic to prevent remote users from introducing vulnerabilities into your network. Cisco AnyConnect delivers optimization for voice with support of Datagram Transport Layer Security (DTLS), and secures third-party endpoints such as Apple iPhones.

Ordering Information

To place an order, visit the Cisco Ordering homepage (http://www.cisco.com/go/ordering) and refer to Tables 2 through 4. To download software, visit the Cisco Software Center (http://www.cisco.com/go/software) You have two options for ordering the Cisco ASA 5500 Series Adaptive Security Appliance to protect your unified communications deployments:

- Option 1: Cisco Unified Communications proxy licenses. You can order Cisco Unified Communications proxy software licenses separately for existing ASA appliances. You can combine features such as phone proxy, mobility proxy, presence federation proxy, and TLS proxy for up to the maximum number of sessions listed in Table 2.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Table 2. Cisco Unified Communications Proxy Maximum Sessions

	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580	Cisco ASA 5585-X SSP-10	Cisco ASA 5585-X SSP-20 or SSP-40 or SSP-60
Unified Communications Proxy Maximum Sessions	24	100	1000	2000	3000	• 5000 for phone proxy • 10,000 for TLS proxy, mobility proxy, presence federation proxy	• 3000 for phone proxy • 3000 for TLS proxy, mobility proxy, presence federation proxy	• 5000 for phone proxy • 10,000 for TLS proxy, mobility proxy, presence federation proxy

- Option 2: Cisco ASA 5500 Series Unified Communications Edition bundles. These appliances bundled with unified communications proxy licenses offer your business a single hardware and software product ID to deliver phone proxy, mobility proxy, presence federation, and TLS proxy features. along with the base firewall and VPN functions. Note that bundles are not available on the ASA 5505, 5510, 5580, or 5585. Please order Unified Communications proxy licenses with ASA hardware. Table 3 provides part numbers.

Table 3. Cisco ASA 5500 Series Unified Communications Edition Ordering Information

Product Name	Part Number
Cisco ASA 5520 Adaptive Security Appliance for Unified Communications Security	
Cisco ASA 5520 Adaptive Security Appliance UC Security Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 1000 UC proxy sessions, 750 IPsec VPN peers, 2 SSL VPN peers, Active/Active and Active/Standby high availability, 3DES/AES	ASA5520-UC-BUN-K9
Cisco ASA 5520 Adaptive Security Appliance UC Security Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 1000 UC proxy sessions, 750 IPsec VPN peers, 2 SSL VPN peers, Active/Active and Active/Standby high availability, 3DES/AES[1]	ASA5520-UC-BUN-K8
Cisco ASA 5540 Adaptive Security Appliance for Unified Communications Security	
Cisco ASA 5540 Adaptive Security Appliance UC Security Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 2000 UC proxy sessions, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES	ASA5540-UC-BUN-K9
Cisco ASA 5540 Adaptive Security Appliance UC Security Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 1000 UC proxy sessions, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES[1]	ASA5540-UC-BUN-K8
Cisco ASA 5550 Adaptive Security Appliance for Unified Communications Security	
Cisco ASA 5550 Adaptive Security Appliance UC Security Edition; includes 8 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 3000 UC proxy sessions, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES	ASA5550-UC-BUN-K9
Cisco ASA 5550 Adaptive Security Appliance UC Security Edition; includes 8 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 1000 UC proxy sessions, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES[1]	ASA5550-UC-BUN-K8

Cisco Unified Communications Services

Cisco Unified Communications Services allows you to accelerate cost savings and productivity gains associated with deploying a secure, resilient Cisco Unified Communications solution. Delivered by Cisco and our certified partners, our portfolio of services is based on proven methodologies for unifying voice, video, data, and mobile applications on fixed and mobile networks. Our unique lifecycle approach to services enhances your technology experience to accelerate true business advantage.

For More Information

For more information about the Cisco ASA 5500 Series or about unified communications on the Cisco ASA platform, visit http://www.cisco.com/go/asa or http://www.cisco.com/go/secureuc. You may also contact your local Cisco account representative.

[1] DES applies to UC licenses in ASA software version 8.2 and earlier. 3DES/AES applies to UC licenses in ASA software version 8.3 and higher

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA C78-450091-03 10/10

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.